

## Construction of Basis Matrices for $(k, n)$ and Progressive Visual Cryptography Schemes

S.B. Bhagate<sup>1\*</sup>, P.J. Kulkarni<sup>2</sup>

<sup>1\*</sup>Department of Computer Science and Engineering, D.K.T.E.'s Textile and Engineering Institute, Ichalkaranji, India

<sup>2</sup>Department of Computer Science and Engineering, Walchand College of Engineering, Sangli, India

\*Corresponding Author: [suhas.bhagate@gmail.com](mailto:suhas.bhagate@gmail.com), Tel.: +91-9860645070

Available online at: [www.ijcseonline.org](http://www.ijcseonline.org)

**Abstract**— Security of digital information plays important role to keep the integrity of original media. A secret is something which is kept away from the knowledge of any but those who are privileged to access it. Secret sharing scheme provides a mechanism for sharing secrets among different users securely, where each user receives his part of encoded secret information called as a share. Sufficient number of shares need to be combined together to reconstruct secret information. Text, images, audio and video can be used for sharing secret information in secret sharing scheme. Secret sharing scheme in which secret information is encoded in form of concealed images is called as Visual Cryptography. There are various Visual Cryptography Schemes. Visual Cryptography Scheme's functionality is dependent on their basis matrices. Constructions of basis matrices for various OR-based and XOR-based Visual Cryptography Schemes are elaborated in this paper.

**Keywords**— Secret sharing scheme, Visual Cryptography, Data hiding

### I. INTRODUCTION

Due to advancements in computing and internet technology, trend of digitizing data and sharing over internet is highly increasing. Internet is a very popular and powerful means of information sharing; however there exists many potential threats. Hackers may attack the weak links over communication network to access unauthorized secret information and misuse the secret information. Information security related issues need to be emphasized while transmitting information over internet. Secret Sharing Schemes handle the issue of illicit usage of information. In 1979, Adi Shamir invented basic secret sharing mechanism [1] and G.R. Blakley invented a mechanism for securing cryptographic keys [2].

When visual secret information like video or image are being shared, that scheme is called as visual secret sharing scheme (VSSS). Visual Cryptography (VC) deals with securing information in form of secret images. Visual Cryptography is a kind of cryptography where visual information is encoded such that decoding can be done without hard computation by human visual system. Fundamental model of visual cryptography is proposed by Moni Naor and Adi Shamir [3], where noise like meaningless shares are created to encode the secret information. Individual shares are not capable of revealing any secret information. Superimposition of all the shares is necessary to reveal secret information.

There is enormous increasing interest in the field of visual cryptography in recent past. Since the origin, many extensions were proposed in order to improve the mechanism of VCS. These extensions to basic visual cryptography scheme (VCS) are (2, 2) Visual Cryptography Scheme,  $(k, n)$  Visual Cryptography Scheme, Multiple Secret Sharing Scheme [4], Extended Visual Cryptography scheme [5], Progressive Visual Cryptography scheme [6] etc. Traditional operation performed while reconstruction of secret image is logical OR operation. It has several limitations. An alternative approach to improve the efficiency of VCS is to use the XOR-based approach [7]. Instead of traditional stacking of the shares, XOR operation will be performed. It improves the overall share quality. XOR-based VCS have merits of good resolution and high contrast [8][9].

In this paper, construction of basis matrices for various Visual Cryptography Schemes like (2, 2) VCS,  $(k, n)$  VCS and Progressive Visual Cryptography scheme (PVCS) by using both OR-based and XOR-based approach are elaborated. Rest of the paper is organized as follows, Section II describes the related work, Section III describes methodology, Section IV describes the experimental result and Conclusion is presented in Section V.

### II. RELATED WORK

In (2, 2) VCS, the given original secret image is encoded into 2 shares. A block of 2 or 4 sub-pixels can be used in each

share to represent the pixels of original secret image. Each share individually does not reveal any secret information. It is necessary to superimpose both the shares to reveal the secret information [3].

Pixels of original secret image can be encoded in different ways. Basis matrices  $S^0$  and  $S^1$  are used for construction of share images. Basis matrix  $S^0$  is used for encoding of white pixels and Basis matrix  $S^1$  is used for encoding of black pixels.

$$S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Figure 1. Basis Matrices for 2 out of 2 Visual Cryptography Scheme

In (2, 2) VCS, each pixel in original secret image is encoded by two sub-pixels in each share. In encoding phase, white pixel in secret image can be encoded by using one of the first two rows in Figure 2. Pixel blocks shown in third and fourth column can be used for encoding the secret in form of two shares. Similarly, black pixel can be encoded using one of the third and fourth rows in figure 2 and corresponding sub-pixel blocks can be assigned to each share.

















Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
	0			
	0			
	1			
	1			

Figure 2. Share Image Construction - (2, 2) Visual Cryptography Scheme

In decoding phase, two shares are superimposed to recover secret image, the result of overlapping will be white pixel when pixel from both the shares overlapped are white. If a black pixel overlaps with either black or white pixel in other share, result of overlapping will be black. The superimposition of shares resembles with logical OR operation. The result of superimposition of sub-pixels of both the shares is shown in last column in Figure 2.

It is mandatory to have both the shares available in (2, 2) VCS to recover secret information. If one of the two shares received is damage or lost, secret information cannot be recovered correctly. So it is must to keep all the shares safe in order to recover the secret and user cannot afford to lose a

single share. To extend the capabilities, basic model of visual cryptography proposed by Naor and Shamir can be generalized into a visual variant of  $k$  out of  $n$  visual cryptography scheme [10]. In  $(k, n)$  VCS, given secret image is encoded into  $n$  shares and distributed among different participants. Any  $k$  out of  $n$  ( $2 \leq k \leq n$ ) shares are necessary to recover the secret image. Any less than  $k$  shares cannot reveal the secret. Secret information can be recovered even some of the shares lost; however minimum  $k$  number of shares must be obtained to recover the secret. General construction of basis matrices for  $(k, n)$  VCS is proposed in section III.

In  $(k, n)$  VCS, all the  $n$  shares created are equally important. Any  $k$  out of  $n$  shares can be used to recover the secret information. There may be a case in which shares can have unequal importance dependent on the user who hold the share. VCS proposed by Ateniese et al deals with this situation [11]. In this scheme, obtained  $n$  shares are classified into two categories namely qualified and forbidden subset of shares by considering importance of the shares. To recover the secret information, any  $k$  shares from qualified subset need to be stacked together. Less than  $k$  shares from qualified subset cannot reveal any secret information. Even more than  $k$  shares from forbidden subset are not capable of revealing any secret information.

In  $(k, n)$  threshold VCS, the secret image can be recovered only by stacking  $k$  or more number of obtained shares. Nothing can be recovered, if there are less than  $k$  overlapped shares. This issue can be handled in progressive visual cryptography scheme proposed by D. Jin, W. Q. Yan, and M. S. Kankanhalli [12]. In progressive visual cryptography scheme (PVCS), it is not mandatory to obtain minimum  $k$  shares out of the  $n$  shares created. Recovery of the secret starts gradually even 2 or more shares obtained. Outline of the secret image will be recovered if only few shares are obtained. More details of hidden secret information can be revealed as more shares stack together. Most realistic recovered image we get, if most of the shares stacked together.

### III. METHODOLOGY

#### A. General Construction of Basis Matrices for $(k, n)$ Visual Cryptography Scheme

In  $k$  out of  $n$  VCS, the given secret image is encoded into  $n$  shares, original secret image can be recovered only if any  $k$  of the  $n$  shares are stacked together. Superimposition of less than  $k$  shares will not reveal any secret information. Each pixel in secret image is encoded in to  $n$  shares using basis matrices  $S^0$  and  $S^1$ . Two Boolean matrices  $S^0$  and  $S^1$  of size  $n \times m$  describes the functionality of visual cryptography scheme. These matrices are called as basis matrices. Black

secret image pixels are encoded by using  $S^0$  and white secret image pixels are encoded by using  $S^1$ .

$$\begin{aligned}
 n &= \text{Number of Rows} = \text{Number of Shares} \\
 m &= \text{Number of Columns} \\
 &= [n! / (k-1)!] / 2 \quad \text{for } (1 < k < n) \\
 &= n \quad \text{if } k = n
 \end{aligned}$$

Matrix  $S^0$  can be constructed in such a way that 1 column has weight  $n$  and remaining  $m-1$  columns have weight 0. Matrix  $S^1$  can be constructed in such a way that all columns have  $(n-k+1)$  number of 1's and  $k-1$  number of 0's.

$$S^0 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad S^1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

Figure 3. Basis Matrices for (3, 4) Visual Cryptography Scheme

Construction of basis matrices for (3, 4) VCS is shown in figure 3. Matrices  $S^0$  and  $S^1$  consist of  $n=4$  rows and  $[n! / (k-1)!] / 2 = 6$  columns. Matrix  $S^1$  used for encoding of white pixels consists of  $(n-k+1) = 2$  number of 1's and  $k-1=2$  number of 0's in each column. While encoding the secret image, if the pixel in original secret image is black, one of the rows from matrix  $S^0$  will be picked up randomly and if the secret image pixel is white, one of the rows from matrix  $S^1$  will be picked up randomly to create shares. Value in first column will be the respective pixel value in share 1, whereas value in second column will be the respective pixel value in share 2 and so on. In decoding phase, respective pixel values will be Ored together to reveal the secret image pixel value. If the secret image pixel value is 1, then at decoding phase result of ORing any 3 shares when stacked together will be 1.

**B. General Construction of Basis Matrices for Progressive Visual Cryptography Scheme**

In Progressive Visual Cryptography Scheme, a given secret image is represented in form of  $n$  shares. Reconstruction of secret image occurs on receiving more than one share gradually. If more number of shares are received, more realistic image gets reconstructed. In this scheme, basis matrix  $S^0$  used for representation of black pixel has one row with values 1 and remaining rows with value 0. It helps to overcome the limitation of disclosing information on shares. If  $S^0$  contain all 0's, then black secret image pixel will be encoded by black pixels in all the shares created. It discloses the secret image data present in form of black pixels. Basis matrix  $S^1$  used for representation of white pixel has diagonal elements with value 1 and remaining elements with value 0. Size of basis matrices  $S^0$  and  $S^1$  is  $n \times n$ .

$$S^0 = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{bmatrix} \quad S^1 = \begin{bmatrix} 1 & 0 & 0 & 0 & \dots \\ 0 & 1 & 0 & 0 & \dots \\ 0 & 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

Figure 4. Basis Matrices for OR-based Progressive Visual Cryptography

In this, secret information is not disclosed on share images, as one row contains all 1's in basis matrix  $S^0$ . At the time of encryption of black pixel, when row with all 1's is picked, represents black secret image pixel with value 1 which represents white pixel. It helps to avoid data disclosure. However it has a limitation by which data recovery is not satisfactory. Recovered image quality is not good compared to original image.

$$S^0 = \begin{bmatrix} 1 & 1 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 0 & 1 & 1 & \dots \\ 0 & 0 & 0 & \dots \\ 1 & 0 & 1 & \dots \\ 0 & 0 & 0 & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix} \quad S^1 = \begin{bmatrix} 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix}$$

Figure 5. Basis Matrices for XOR-based Progressive Visual Cryptography

Good quality images can be recovered by using XOR-based reconstruction approach. Basis matrices are modified so that XOR based reconstruction approach can be implied. In this scheme basis matrices  $S^0$  and  $S^1$  will have size of  $n \times (n-1)$  rows and  $n$  columns. Basis matrix  $S^0$  used for representation of black pixel has  $n \times (n-1) / 2$  rows with combinations of two 1's and remaining all 0's. Other  $n \times (n-1) / 2$  rows have all 0 values. Basis matrix  $S^1$  used for representation of white pixel has diagonal elements with value 1 and remaining elements with value 0. Such  $(n-1)$  groups are present in basis matrix  $S^1$ . This approach has obvious merit of higher data recovery in terms of PSNR. Recovered image looks more alike original image still secret information is not disclosed on share images. Each secret image pixel is represented by only 1 pixel in all share images. So there is no pixel expansion in this proposed approach, which is advantageous. It saves the space and network bandwidth while transmitting shares in network.

#### IV. RESULTS AND DISCUSSION

We implemented OR-based Progressive Visual Cryptography Scheme and proposed XOR-based Progressive Visual Cryptography Scheme by using Java SE Development Kit 8u151 in a personal computer running MS Windows 8.1 with CPU Intel® Core™ 2 Duo 2.2 GHz and a memory of 4 GB. Viability of XOR-based VCS is indicated by following experimental results. We have experimented on an image with a size of 256×256, shown in Fig. 6.



Figure 6. Original Secret Image

While encoding the secret image in OR-based Progressive Visual Cryptography Scheme, basis matrices shown in figure 4 have been used and for XOR-based Progressive Visual Cryptography Scheme, basis matrices shown in figure 5 have been used. In our example five shares are created of original Secret Image using basis matrices. Size of basis matrices is 5X5. If the secret image pixel is black, one of the rows from matrix  $S^0$  is picked up randomly and if the secret image pixel is white, one of the rows from matrix  $S^1$  is picked up randomly to create shares. Value in first column is the respective pixel value in share 1, value in second column is the respective pixel value in share 2 and so on. In decoding phase, reconstruction is done by using any of 2 shares, 3 shares, 4 shares or by using all 5 shares. In this phase respective pixel values will be XORed together to reveal the secret image pixel value. If the XORed value is 0 then the recovered pixel will be black and if the XORed value is 1 then the recovered pixel will be white.

Figure 7 shows the reconstruction of secret image in OR-based Progressive Visual Cryptography Scheme (PVCS).

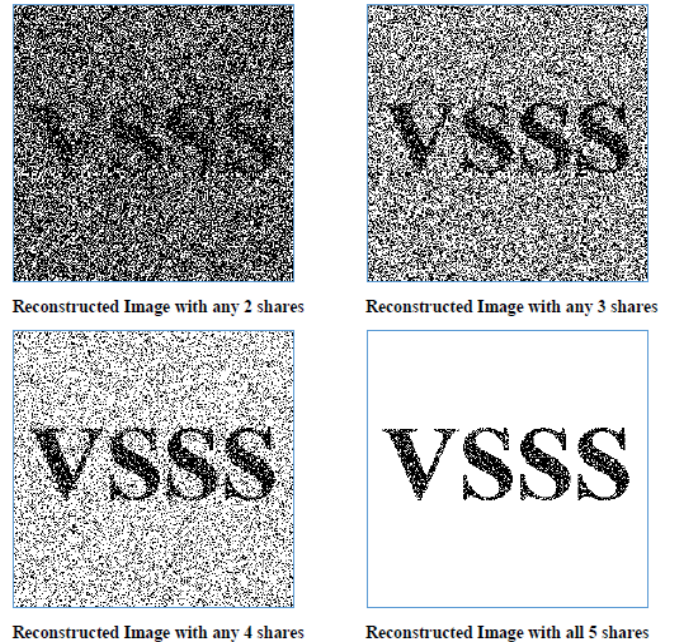


Figure 7. Reconstruction of Secret Image using OR-based PVCS

Figure 8 shows the reconstruction of secret image in XOR-based Progressive Visual Cryptography Scheme (PVCS).

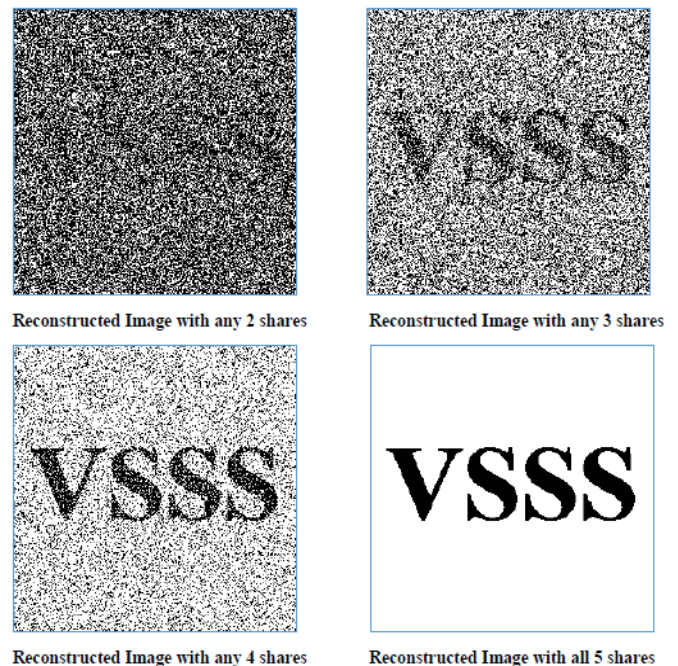


Figure 8. Reconstruction of Secret Image using XOR-based PVCS

Peak Signal to Noise Ratio (PSNR) of all the reconstructed images when compared to original secret image are shown in table 1.

Table 1. PSNR of Reconstructed Images

No. of shares used for Reconstruction	PSNR	
	OR-based Progressive Visual Cryptography Scheme	XOR-based Progressive Visual Cryptography Scheme
2	4.86	4.90
3	8.22	8.34
4	13.96	14.08
5	33.24	50.72

## V. CONCLUSION and Future Scope

Progressive Visual Cryptography can recover secret image gradually with availability of more number of shares. Reconstructed image quality is poor in OR-based PVCS. This is overcome in XOR-based PVCS proposed in this paper. XOR-based PVCS has merit of higher data recovery in terms of PSNR. Recovered image looks more alike original image still secret information is not disclosed on share images. One of the issues required to be handled further is to consider noise like shares which may arouse the attention of hacker. Extended VCS can be used to create meaningful shares and handling issue of noise like shares.

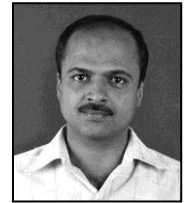
## REFERENCES

- [1] Shamir, A. 1979. How to Share a Secret. Communications of the ACM. 22: 612-613.
- [2] Blakely, G. R. 1979. Safeguarding Cryptographic Keys. Proceedings of the National Computer Conference, American Federation of Information Processing Societies Proceedings. 48: 313-317.
- [3] Moni Naor and Adi Shamir, "Visual cryptography". In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.
- [4] S. J. Shyu, S. Y. Huang, Y. K. Lee, R. Z. Wang, and K. Chen, "Sharing multiple secrets in visual cryptography", Pattern Recognition, Vol. 40, Issue 12, pp. 3633 - 3651, 2007.
- [5] Nakajima, M. and Yamaguchi, Y., "Extended visual cryptography for natural images" Journal of WSCG. v10 i2. 303-310.
- [6] Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, pp. 1-13, 2005.
- [7] Pim Tuyls, Henk D. L. Hollmann, Jack H. van Lint, and Ludo M. G. M. Tolhuizen. XOR-based visual cryptography schemes. Designs, Codes and Cryptography, 37(1):169-186, 2005
- [8] C.-N. Yang and D.-S. Wang, "Property analysis of XOR-based visual cryptography," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 24, no. 2, pp. 189-197, Feb. 2014.
- [9] X. Wu and W. Sun, "Extended capabilities for XOR-based visual cryptography," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1592-1605, Oct. 2014.
- [10] E. Verheuland H. V. Tilborg, "Constructions And Properties Of K Out Of N Visual Secret Sharing Schemes." Designs, Codes and Cryptography, 11(2), pp.179-196, 1997.

- [11] G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, "Visual cryptography for general access structures", Proc. ICAL96, Springer, Berlin, 1996, pp.416-428.
- [12] Jin, W. Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," J. Electron. Imag., vol. 14, no. 3, pp. 1-13, 2005.

## Authors Profile

*Mr. Suhas B. Bhagate* pursued Bachelor of Engineering from Shivaji University, Kolhapur in 2003 and Master of Engineering from Walchand College of Engineering, Sangli in Shivaji University, Kolhapur in year 2011. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science and Engineering, D.K.T.E. Society's Textile and Engineering Institute, Ichalkaranji since 2004. He is IEEE Graduate Student Member. He has published more than 10 research papers in reputed international journals. His main research work focuses on Visual Cryptography Algorithms, Data Structures, Big Data Analytics and Data Mining.



*Dr. Prakash Jayant Kulkarni* pursued Bachelor of Engineering from University of Poona in 1979, Master of Engineering in the subject Digital Signal Synthesis from Shivaji University, Kolhapur in 1986, and Ph.D. in Electronics in the subject Digital Image Processing from Shivaji University, Kolhapur in 1993. He is currently working as Professor in Computer Science and Engineering Dept., Walchand College of Engineering, Sangli. He has provided guidance to many PhD students in the areas of Electronics Engineering and Computer Science and Engineering. He has executed many research proposals of AICTE, New Delhi. His research interest includes Computer Vision, Pattern recognition, Artificial Neural Networks, Data Mining, Web mining and Information retrieval. He is also a recipient of Best Teacher Award of Maharashtra State Government for the year 2011-2012.

